

中文引用格式:任杰,曲仕茹,王莉莉,等. 基于 STPA-BN 的真北导航过渡风险评估模型[J]. 中国安全科学学报,2026,36(5):165-173.
英文引用格式:Ren Jie, Qu Shiru, Wang Lili, et al. Risk assessment model for true north transition in aviation based on STPA-BN [J].
China Safety Science Journal,2026,36(5):165-173.

基于 STPA-BN 的真北导航过渡风险评估模型^{*}

任杰^{1,2}讲师,曲仕茹²教授,王莉莉¹教授,韩元松¹,孙志远¹

(1 中国民航大学 空中交通管理学院,天津 300300; 2 西北工业大学 自动化学院,陕西 西安 710072)

中图分类号:X949

文献标志码:A

DOI:10.16265/j.cnki.issn1003-3033.2026.05.0952

基金项目:中央高校自然科学一般项目(3122024042);天津市自然科学基金联合基金面上项目资助(25JCLMJC00530)。

【摘要】 随着全球民航导航系统向以真北为基准的导航方式转型,为量化识别与有效控制导航基准转换所引发的系统性风险,提出一种融合系统理论过程分析(STPA)与模糊贝叶斯网络(FBN)的动态风险评估模型,用于支持真北导航过渡过程中的多源不确定性风险识别与演化分析,构建包含“战略-区域-组织-设备”4层次的控制结构,系统识别7类系统级危险与12项不安全控制行为(UCA),并通过模糊集方法处理专家认知的不确定性,结合 Leaky Noisy-or 门逻辑建立贝叶斯网络(BN),进一步扩展为动态贝叶斯网络(DBN)模拟5阶段($t_0 \sim t_0+28$ 年)风险演化过程。结果表明:技术适配滞后与政策协同不足是初期主要风险驱动因素(如空域冲突概率达0.852),但通过分阶段推进技术升级、政策协调与冗余设计,关键风险在 t_0+28 年可降低至0.01以下。研究提出融合“阶段达标-资金拨付”政策联动机制、基于机型寿命分级的技术迭代路径以及“惯导+低轨卫星”双冗余人工智能(AI)治理体系的原创策略,以系统性解决真北过渡中的政策延迟、设备代际冲突及运行风险问题。

【关键词】 系统理论过程分析(STPA); 模糊贝叶斯网络(FBN); 真北导航; 风险评估; 不安全控制行为(UCA); 过渡过程; 风险缓解

Risk assessment model for true north transition in aviation based on STPA-BN

Ren Jie^{1,2}, Qu Shiru², Wang Lili¹, Han Yuansong¹, Sun Zhiyuan¹

(1 School of Air Traffic Management, Civil Aviation University of China, Tianjin 300300, China;

2 School of Automation, Northwestern Polytechnical University, Xi'an Shaanxi 710072, China)

Abstract: With the global transition of civil aviation navigation systems from magnetic north to true north reference, a dynamic risk assessment model integrating STPA and FBN was proposed to quantify, identify, and effectively control systemic risks induced by the navigation reference transition. A four-level control structure-covering strategic, regional, organizational, and equipment layers-was established to identify seven categories of system-level hazards and twelve types of unsafe control actions. Expert uncertainty was quantified via fuzzy sets, and a Bayesian network (BN) was constructed using the Leaky Noisy-or Gate model. Furthermore, a dynamic Bayesian network (DBN) was developed to simulate risk evolution across five phases (t_0 to t_0+28 years). The results show that technological lag and insufficient

policy coordination are the major risk drivers in the early stage (e.g., airspace conflict probability up to 0.852). However, through phased implementation of technology upgrades, policy alignment, and redundancy design, key risks can be reduced to below 0.01 by $t_0 + 28$. This study proposes an original strategy integrating the ‘phased compliance-fund disbursement’ policy linkage mechanism, aircraft service life-based technical iteration path, and the ‘inertial navigation + low-orbit satellite’ dual-redundancy artificial intelligence (AI) governance system, to systematically resolve policy delays, intergenerational equipment conflicts and operational risks in the true north transition.

Keywords: system-theoretic process analysis (STPA); fuzzy Bayesian network (FBN); true north navigation; risk assessment; unsafe control action (UCA); transition process; risk mitigation

0 引言

随着全球民航业的快速发展,航空导航系统对精度、稳定性及跨区域兼容性的要求不断提高。传统以磁北为基准的导航体系受地磁偏角时空变化及测量误差限制,已难以满足高精度运行需求,尤其在极地、海洋等磁异常区域表现更为突出。近年来,全球卫星导航系统(Global Navigation Satellite System, GNSS)的普及使得以真北为基准的导航成为可能。真北导航具有坐标稳定、全球一致、不受地磁扰动影响等优势,已在海事和部分航空场景中展现出显著技术潜力^[1]。国际民航组织(International Civil Aviation Organization, ICAO)已成立真北咨询小组(True North Advisory Group, True-AG),积极推动全球向真北基准过渡^[2]。然而,这一转型不仅是技术标准的更新,更涉及空管运行、飞行程序、机载设备、人员培训及跨国协调等多维度系统性变革,亟需开展系统化、前瞻性的安全风险评估,以保障过渡过程的安全、有序与高效^[3]。

当前,针对复杂系统安全风险的识别与建模,系统理论过程分析(System-Theoretic Process Analysis, STPA)因其能有效揭示控制结构中的不安全控制行为(Unsafe Control Action, UCA)而被广泛应用于航空安全领域。Abdulkhaleq等^[4]验证了STPA在软件密集型系统中的适用性;Krauss等^[5]探讨了其在航空系统中的工具支持与验证路径;Sahay等^[6]通过对比安全STPA、信息安全威胁分析和风险评估与基于模型的风险评估3种方法,进一步肯定STPA在早期风险干预中的优势。然而,STPA在风险量化与动态演化建模方面存在局限。为弥补此不足,研究者尝试将STPA与贝叶斯网络(Bayesian Network, BN)融合。Basnet等^[7]在远程引航场景中构建了从UCA到BN的转化框架;张子昂等^[8]引入

模糊BN(Fuzzy BN, FBN),实现了对“人-机-环”多维风险的量化评估;王洁宁等^[9]将该方法应用于空管自动化系统的人因失误分析。尽管如此,现有方法在处理模糊不确定性、动态时序演化及多层级控制耦合方面仍有待深化。此外,席永涛^[10]、Li Wei^[11]、Lu Xin^[12]等分别将STPA与模糊时序Petri网、蒙特卡罗模拟及扩展BN相结合,探索了在船舶等复杂动态系统中的实时或演化风险评估。张玉磊等^[13]强调多方协同机制对重大技术转型的重要性;门茂林等^[14]从测量角度验证了真北系统的精度优势,为过渡提供技术支撑。综上,上述研究尚未形成覆盖全链条的动态风险评估体系^[15-16]。

鉴于此,笔者拟提出一种融合STPA与FBN的动态风险评估模型,并在此基础上构建5阶段动态BN(Dynamic BN, DBN),用以模拟真北导航运行过渡过程中关键风险的演化趋势,以期为全球真北导航过渡提供一套可量化、可追溯、可预测的风险评估方法,支撑安全规划、资源配置与协同决策。

1 基于STPA-BN的真北导航过渡风险评估模型

为系统识别真北导航过渡过程中的控制链缺陷与潜在风险路径,实现不确定性条件下的定量推理,提出一种融合STPA与FBN的集成建模方法。STPA用于提取系统中的UCAs及其触发条件,FBN对系统风险传播过程进行量化建模,为后续的动态风险评估与敏感性分析提供建模基础。

1.1 基于STPA的系统风险识别

STPA由Leveson提出,是一种基于系统控制结构和行为约束的安全分析方法,适用于复杂系统的潜在风险识别。STPA通过建模系统的控制结构,识别UCAs并推导其触发条件,从而构建事故因果

链。其典型流程包括系统建模、危险识别、控制行为分析和原因分析 4 个步骤,适用于识别真北导航过渡中的多源风险和结构化表达。

1.1.1 定义系统边界目标

在 ICAO 框架下,定义真北过渡系统目标为建立覆盖“政策-技术-操作”全链条的协同体系,核心约束条件包括:

- 1) 政策法规约束,ICAO 标准更新周期差异,各国政策执行效率不均。
- 2) 利益协同约束,需协调军方、原始设备制造商、飞机制造商、航空公司、空管、机场等多方利益。
- 3) 技术兼容约束,需规避导航数据库更新周期差异导致的数据断层风险。
- 4) 经济成本约束,主要涉及航电设备、航空器升级改造及跑道标志更新的成本。
- 5) 空管运行约束,空管自动化系统需实现对磁/真航向混合指令的解析,控制管制员认知负荷的增长。
- 6) 环境约束,极地 GNSS 信号覆盖薄弱,需应对太阳耀斑干扰及恶意欺骗风险。

1.1.2 分层控制结构建模

借鉴 ICAO True-AG 提出的全球过渡结构框架,构建覆盖“战略规划-区域协调-组织实施-设备操作”4 层控制结构,如图 1 所示,用于系统性识别控制链中潜在安全失效路径。

1.1.3 系统级危险(Hazards)识别

结合分层结构控制建模,识别出 7 类关键系统级危险,并依据 ICAO 风险等级标准设定严重性等级,见表 1。

表 2 UCAs 与危险映射
Table 2 Mapping of UCAs to hazards

控制行为	UCA 类型	不安全场景	触发条件	关联危险
政策制定滞后	未提供	缺乏实施细则,无法启动设备/系统设计改造	政策协调效率<50%	H-1
改装方案不兼容	错误提供	硬件冲突,设备运行不稳定	未纳入老旧机型替换协议	H-2
提前进入真北运行	时机错误	混合运行未验证,空管指令解读混乱	空管培训覆盖率<80%,技术验证不足	H-3
数据维护延迟	持续时间不当	导航数据库过期,航图与运行不一致	数据提供商资源调配不足	H-4
缺乏改造补贴	未提供	企业因成本过高推迟改造计划	财政预算未设专项资金	H-5
导航设施校准误差	参数错误	误差超限,影响运行精度	校准工具缺失或培训不足	H-2/H-6
备份激活失败	持续时间不当	GNSS 失效未能及时激活惯导备份	应急程序机制缺失,测试覆盖不足	H-7

1.1.5 STPA 到 BN 的转化逻辑

为将 STPA 的定性分析结果转化为可定量计算的 BN 模型,遵循以下映射规则:

- 1) BN 节点。对应于 STPA 分析中的 UCAs 的

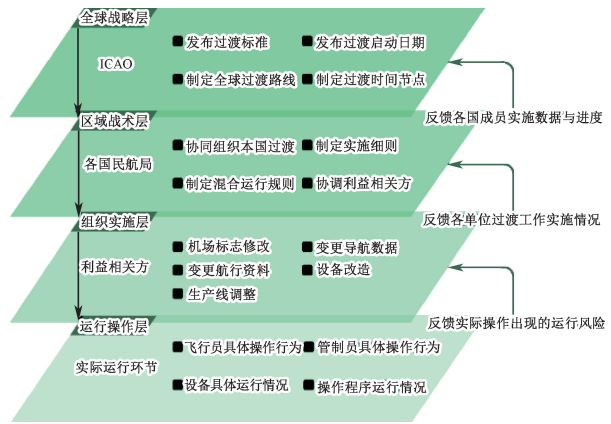


图 1 真北过渡分层控制结构
Fig.1 Hierarchical control structure of true north transition

表 1 系统级危险识别结果
Table 1 System-Level Hazards Identification

编号	危险类别	危险描述	严重性等级
H-1	政策协同风险	各国过渡政策不统一	3 级
H-2	技术适配风险	老旧设备无法支持真北运行	2 级
H-3	空管混合运行风险	磁/真双基准指令混乱	3 级
H-4	数据断层风险	导航数据库更新周期差异	2 级
H-5	经济超支风险	设备改造成本超标	2 级
H-6	人为失误风险	飞行员误读航图	2 级
H-7	环境干扰风险	GNSS 信号受太阳耀斑干扰	3 级

1.1.4 UCAs 分析

依照 STPA 的 4 类 UCA 类型,结合触发条件与已识别危险事件,系统分析各类 UCAs,并建立危险映射,见表 2。

表 2 UCAs 与危险映射
Table 2 Mapping of UCAs to hazards

控制行为	UCA 类型	不安全场景	触发条件	关联危险
政策制定滞后	未提供	缺乏实施细则,无法启动设备/系统设计改造	政策协调效率<50%	H-1
改装方案不兼容	错误提供	硬件冲突,设备运行不稳定	未纳入老旧机型替换协议	H-2
提前进入真北运行	时机错误	混合运行未验证,空管指令解读混乱	空管培训覆盖率<80%,技术验证不足	H-3
数据维护延迟	持续时间不当	导航数据库过期,航图与运行不一致	数据提供商资源调配不足	H-4
缺乏改造补贴	未提供	企业因成本过高推迟改造计划	财政预算未设专项资金	H-5
导航设施校准误差	参数错误	误差超限,影响运行精度	校准工具缺失或培训不足	H-2/H-6
备份激活失败	持续时间不当	GNSS 失效未能及时激活惯导备份	应急程序机制缺失,测试覆盖不足	H-7

触发条件(视为风险根源,即父节点)、Hazards(视为中间风险状态,即中间节点)以及可能引发的最终事故(视为后果,即子节点)。

- 2) 依赖关系。BN 中的有向边反映了 STPA 中

已识别的因果关系。如一个UCA(如“政策制定滞后”)可能触发多个危险(如H-1政策协同风险),一个危险(如H-2技术适配风险)也可能由多个UCA(如改装方案不兼容、导航设施校准误差)共同导致。这种多对多的因果映射关系通过BN的网状结构得以精确表达。

3) 条件概率表(Conditional Probability Table, CPT)量化了父节点对子节点的影响强度,其构建基于STPA中分析的UCA触发场景和专家知识。Leaky Noisy-OR模型的引入,特别适用于描述多个父节点(原因)中任一发生都可能以一定概率导致子节点(结果)发生的情况,这与STPA中多种失效路径导致同一危险的分析逻辑高度契合。

通过转化规则,STPA所揭示的系统性、交互性风险路径被系统地编码为BN的拓扑结构和参数,实现了从定性系统分析到定量概率推理的无缝衔接。

1.2 FBN 模型构建

BN是一种基于概率推理的图模型,能够描述变量之间的因果关系并进行不确定性分析。为适应专家判断中的语言模糊性,引入FBN方法,在保留贝叶斯条件推理优势的基础上,增强模型对专家主观意见的量化表达能力。

1.2.1 节点与结构定义

基于1.1.5节的转化逻辑,将STPA输出映射为BN节点,拓扑结构如图2所示。

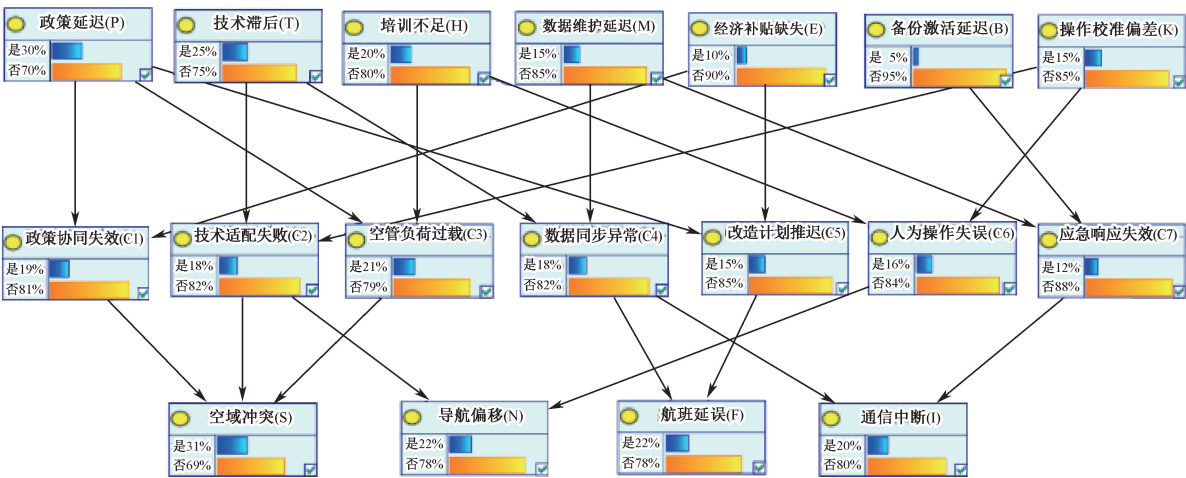


图2 BN 拓扑结构(GeNIe 构建)

Fig. 2 BN topology (constructed in GeNIe)

1) 父节点,7项UCAs触发条件见表3。

表3 父节点定义

Table 3 Parent nodes of BN

节点名称	对应UCA类型	关联危险
政策延迟 <i>P</i>	未提供(政策制定滞后)	H-1
技术滞后 <i>T</i>	错误提供(设备改装不兼容)	H-2
培训不足 <i>H</i>	时机顺序错误(提前进入真北运行)	H-3
数据维护延迟 <i>M</i>	持续时间不当(数据维护延迟)	H-4
经济补贴缺失 <i>E</i>	未提供(经济补贴缺失)	H-5
操作校准偏差 <i>K</i>	参数错误(操作校准偏差)	H-2/H-6
备份激活延迟 <i>B</i>	持续时间不当(备份系统激活延迟)	H-7

2) 中间节点,7类系统危险见表4。

表4 中间节点定义

Table 4 Intermediate nodes of BN

节点名称	风险传播路径	新增关联UCA
政策协同失效 <i>C₁</i>	<i>P</i> + <i>E</i>	未提供类UCA双重影响
技术适配失败 <i>C₂</i>	<i>T</i> + <i>K</i>	错误提供+参数错误类UCA叠加
空管负荷过载 <i>C₃</i>	<i>H</i> + <i>P</i>	时机顺序错误+未提供类UCA关联
数据同步异常 <i>C₄</i>	<i>M</i> + <i>T</i>	持续时间不当+错误提供类UCA耦合
改造计划推迟 <i>C₅</i>	<i>E</i> + <i>P</i>	未提供类UCA联合影响
人为操作失误 <i>C₆</i>	<i>K</i> + <i>H</i>	参数错误+时机顺序错误类UCA交织
应急响应失效 <i>C₇</i>	<i>B</i> + <i>M</i>	持续时间不当类UCA叠加影响

3) 子节点,4 类事故见表 5。

表 5 子节点(事故类型)定义

Table 5 Child nodes (consequence events) of BN			
节点名称	核心触发路径	关联危险组合	严重性等级
空域冲突 S	C_3+C_2	H-2+H-3	3 级(高)
通信中断 I	C_4+C_7	H-4+H-7	2 级(中)
航班延误 F	C_5+C_4	H-4+H-5	1 级(低)
导航偏移 N	C_6+C_2	H-2+H-6	2 级(中)

1.2.2 模糊概率赋值

采用“高、中、低”3 级梯形模糊数构建模糊数转化专家判断,通过重心法解模糊,得到精确概率值。高、中、低对应的梯形模糊数分别为(0.7,0.8,0.9,1.0)、(0.4,0.5,0.6,0.7)、(0.1,0.2,0.3,0.4),解模糊值依次为 0.85、0.55、0.25。

组织 15 名涵盖 ICAO 政策、原始设备制造商(Original Equipment Manufacturer, OEM)技术、空管运行等领域的专家,按 30%、25%、20%、15%、10% 的权重分配意见。依据专家权重采用加权平均法整合意见,确定父节点最终概率,见表 6。

1.2.3 CPT 构建

采用 Leaky Noisy-OR 逻辑函数设置中间节点与子节点的条件概率,泄露概率设为 $P_L=0.10$,以此表征未知因素。

表 7 父节点概率阶段调整策略及依据

Table 7 Stage-wise probability adjustment of parent nodes and rationale

阶段	政策延迟概率	技术滞后概率	阶段特征与优化措施
t_0 阶段 (决策基准年)	0.30	0.25	启动阶段,初始不确定性高。设立启动基金,制定初步过渡计划。风险主要源于政策意向和技术可行性的初始不确定性
t_0+5 阶段 (标准生效期)	0.40→0.20	0.50→0.15	国际标准生效,执行挑战显现。初期各国协调复杂度高,政策风险上升;大规模技术改造启动,技术问题集中暴露(T 先升)。随着协调机制建立和技术问题被攻克,期末 2 项风险均显著下降
t_0+10 阶段 (首区过渡期)	0.30→0.10	0.35→0.05	示范效应显现,学习曲线加速。首批地区实现全面“真北”运行,其成功经验为全球政策协调提供动力(P 降),并促进技术方案的标准化和成熟化(T 降)
t_0+20 阶段 (过渡完成期)	0.10→0.05	0.15→0.01	全球切换基本完成,系统趋于稳定。超过 90% 的空域已完成切换,混合运行场景急剧减少。政策和技术层面的系统性风险已得到有效控制,降至很低水平
t_0+28 阶段 (自然淘汰期)	0.05→0.01	0.05→0.01	系统进入稳态,残余风险极低。依赖“磁北”的老旧设备已自然淘汰殆尽,“真北”成为唯一基准。系统进入长期稳态运行,残余风险接近可忽略水平

1) t_0 (决策基准年),全球达成过渡共识,制定初步路线。政策和技术风险主要源于不确定性和初始准备不足。

2) t_0+5 (标准生效期),ICAO 标准正式生效,各国开始修订法规。政策延迟风险因协调复杂度可能

表 6 父节点概率赋值结果

Table 6 Probability values of parent nodes

节点名称	状态	模糊判断	解模糊值	最终概率
P	是	中	0.25	0.30
T	是	低	0.25	0.25
H	是	中低	0.45	0.20
M	是	低	0.25	0.15
E	是	低	0.25	0.10
K	是	中高	0.55	0.15
B	是	低	0.25	0.05

1.3 DBN 扩展

为捕捉真北过渡这一长期动态过程中的风险演化特征,将静态 BN 扩展为 DBN。过渡过程并非瞬时切换,而是涉及政策逐步落地、技术迭代更新、人员适应培训的漫长时序过程,期间风险驱动因素的强度和各因素间的相互作用会随时间变化。

1.3.1 阶段划分与参数设定

依据 ICAO True-AG 初步确定的过渡路线图及其内在逻辑(政策从制定到生效的延迟、技术从研发到普及的周期、人员从培训到熟练的过程),构建 5 阶段 DBN 模型,各阶段特征与父节点概率调整策略见表 7。

先期升高,技术滞后风险因改造工作启动而显现。

3) t_0+10 (首区过渡期),部分条件成熟的地区(如高纬度国家)率先完成过渡,积累经验。政策和技术风险因局部成功而开始显著下降。

4) t_0+20 (过渡完成期),全球绝大多数空域完

成切换,新旧系统混合运行范围大幅缩小。主要风险因素得到有效控制。

5) t_0+28 (自然淘汰期),支持磁北的老旧设备已基本被淘汰,真北运行成为绝对主导。系统进入稳定运行状态,残余风险极低。

1.3.2 风险演化模拟

通过 GeNIe 平台模拟风险概率变化,子节点风险随阶段概率演化趋势见表 8。

表 8 子节点风险演化特征

Table 8 Evolution of consequence node probabilities across stages				
阶段	空域冲突	通信中断	航班延误	导航偏移
t_0	0.852	0.626	0.707	0.684
t_0+5	0.484	0.374	0.300	0.250
t_0+10	0.200	0.150	0.100	0.080
t_0+20	0.050	0.030	0.020	0.010
t_0+28	0.010	0.005	0.002	0.001

由表 8 可知:通过阶段性政策推进与技术干预,关键风险(如空域冲突)将从 0.852 降至 0.01 以下。该演化趋势清晰地反映过渡过程早期因系统交互和不确定性导致的高风险,以及中后期随着控制措施逐步生效、系统趋于稳定而风险显著降低的动态特征。模型在动态场景中响应合理、结构完备,验证了其作为真北过渡风险演化建模工具的实用性与可靠性。

2 真北导航过渡 STPA-FBN 模型验证与风险评估

2.1 STPA-FBN 动态风险模型验证设计

由于当前缺乏实际的历史数据,通过模拟不同假设场景进行模型验证。尽管无法直接对比历史数据中的场景,设定多个理论情景,并将其输入到模型中,检查模型的输出结果与预期的风险等级是否一致。此外,考虑到多源不确定性,模型进一步利用专家赋值与 FBN 的组合,提供了可靠的风险评估和预测能力。为验证所构建 STPA-FBN 动态风险评估模型的结构合理性与推理有效性,从逻辑结构、正向/反向推理准确性、敏感性响应及专家数据可信度 4 个维度开展模型验证分析,确保模型在航空系统实际应用中的可靠性与解释能力。

2.1.1 逻辑完备性验证

模型的结构合理性是进行有效推理的基础。首先,利用 GeNIe 软件对构建的 BN 结构进行严格的有向无环图检验,确认所有节点间的因果关系均为

单向传递,不存在循环依赖路径,符合因果推理的基本逻辑要求。其次,应用拓扑排序算法遍历网络中的所有节点,验证了其依赖关系的单向性和无环性,彻底排除了形成逻辑闭环的可能性。最后,归一化检验模型中所有节点的 CPT。通过计算每一组父节点状态组合下子节点所有状态的概率和,确保其严格等于 1(允许 ± 0.001 的数值计算误差)。如空域冲突(S)节点的 CPT 在 8 种父节点状态组合下,其“是”与“否”状态的概率和均精确为 1.000。这一系列严谨的检验过程,从结构拓扑和数值逻辑 2 个层面,保证了模型内在逻辑的严密性和一致性,为后续的定量推理奠定了坚实的数学基础。

2.1.2 正向推理验证

目标是验证模型在输入高风险父节点时,输出结果是否与理论预期一致,体现模型的推理准确性与多源耦合响应能力。

设定高风险场景政策延迟 P 概率为 0.8、技术滞后 T 概率为 0.7,其他节点保持默认值,模型输出概率为 0.92,误差率仅 1.09%,验证了模型的推理准确性和多源耦合响应能力。

2.1.3 反向推理验证

通过强制设定子节点状态并推导父节点后验概率,验证模型的诊断能力和因果链闭环完整性。

设定空域冲突(S)=是,观察 P 、 T 等父个节点的后验概率变化。结果显示, P 后验概率从 0.30 上升至 0.42, T 后验概率从 0.25 上升至 0.29。这种后验概率的上升清晰地表明:当观测到“空域冲突”这一严重后果发生时,模型能够合理地将风险源头指向政策协同和技术适配这 2 个在 STPA 分析中识别出的核心 UCAs(未提供、错误提供)。这种诊断结果与真北过渡中政策标准不统一、老旧设备兼容性差是冲突主要诱因的认知完全一致。该验证成功证明了模型具备闭环的因果诊断能力,能够为事故调查和风险源头识别提供有力的量化支持。

2.1.4 敏感性分析

敏感性分析用于量化评估输入参数(父节点概率)变动对模型输出结果(子节点概率,尤其是关键事故风险)的影响程度,从而识别出最关键的风险驱动因子。采用标准化敏感系数(Standardized Influence, SI)作为衡量指标。SI 值越高,表明该父节点概率的波动对目标风险(如航班延误 F)的影响越大,其风险驱动作用越强。敏感性分析显示,技术滞后(SI=0.82)为核心风险驱动因素,政策延迟(SI=0.55)为次要驱动,培训不足(SI=0.18)影响

较弱。

2.1.5 专家数据可信度分析

为加强模型量化基础的可信度,对采用的专家数据进行以下检验:

- 1) 数据来源。所有概率数据均为 15 人专家小组,覆盖政策、技术、运行等关键领域,具有代表性。
- 2) 数据处理。采用模糊德尔菲法整合专家意见,首先,收集专家对父节点发生可能性的模糊语言评价(高/中/低);然后,利用模糊数和解模糊方法将语言评价转化为精确值;最后,根据专家权重进行加权平均,得到最终的先验概率赋值。此过程有效降低了专家判断的主观性和不确定性。
- 3) 信度检验。为评估专家意见的一致性,计算专家评价的克隆巴赫 α (Cronbach's α) 系数。经计算, $\alpha=0.78(>0.7)$,表明专家评价结果具有良好的内部一致性信度,支持了所用数据的可靠性。

3 真北导航过渡风险量化评估与缓解

基于经过严格验证的 STPA-FBN-DBN 模型,系统地量化评估真北运行过渡过程中的风险,并依据评估结果,针对性地提出多维度、系统性的风险缓解策略。量化分析不仅揭示了当前风险水平,更通过动态模拟展示了风险随缓解措施推进的长期演化趋势,为过渡路径的优化和安全决策提供科学支撑。

3.1 风险评估量化分析

3.1.1 风险值计算与风险等级划分

结合模型输出概率与风险严重性等级(表 1),采用风险矩阵法[风险度(Risk Level, RV)= 概率 p × 严重性 s]划分风险等级。依据 ICAO 风险分级标准,将风险划分为:极低风险($RV < 0.5$):可接受;低风险($0.5 \leq RV < 1.0$):常规监测;中风险($1.0 \leq RV < 2.0$):需制定缓解措施;高风险($RV \geq 2.0$):需立即干预。

量化关键风险节点的结果见表 9。

表 9 关键节点风险量化值

Table 9 Risk quantification of key nodes				
节点	p	s	RV	风险等级
C_2	0.35	3(高)	1.05	中风险
C_1	0.41	3(高)	1.23	中风险
C_3	0.57	2(中)	1.14	中风险
C_7	0.27	3(高)	0.81	低风险
S	0.352	3(高)	1.06	中风险
I	0.374	2(中)	0.75	低风险
N	0.484	2(中)	0.97	低风险

3.1.2 动态风险演化分析

结合 DBN 五阶段模型,追踪风险在真北过渡过程中随时间的动态变化趋势,各阶段关键风险指标演化见表 10。该演化过程清晰地模拟了政策和技术这 2 个核心驱动因素在各阶段受不同措施影响而变化,进而导致系统风险状态随之演进的连锁反应。

表 10 关键风险指标动态演化

Table 10 Dynamic evolution of key risk indicators			
阶段	C_2	C_1	S
t_0 阶段 (决策基准年)	$p=0.35$, $RV=1.05$	$p=0.41$, $RV=1.23$	$p=0.852$
t_0+5 阶段 (标准生效期)	$p=0.15$, $RV=0.45$	$p=0.20$, $RV=0.60$	$p=0.484$
t_0+10 阶段 (首区过渡期)	$p=0.05$, $RV=0.15$	$p=0.10$, $RV=0.30$	$p=0.200$
t_0+20 阶段 (过渡完成期)	$p=0.01$, $RV=0.03$	$p=0.05$, $RV=0.15$	$p=0.050$
t_0+28 阶段 (自然淘汰期)	$p=0.01$, $RV=0.03$	$p=0.01$, $RV=0.03$	$p=0.010$

- 1) t_0 阶段。政策 P 概率为 0.30 和技术 T 概率为 0.25 风险处于中等水平,但因系统间紧密耦合和初始的不确定性,导致空域冲突 S 概率为 0.852 等后果风险极高。这揭示了复杂系统转型初期的典型特征-局部风险可能通过交互作用被放大为全局高风险。
- 2) t_0+5 阶段。随着标准生效和改造启动,协调难题和技术挑战集中暴露, P 和 T 概率一度升高。但由于应对措施已开始实施,期末空域冲突 S 概率为 0.484 较 t_0 阶段已显著下降,表明控制措施开始生效。
- 3) t_0+10 及以后阶段。随着试点成功经验推广、设备更新范围扩大、人员熟练度提升, P 和 T 概率持续下降,系统各节点风险值随之稳步降低。至 t_0+28 阶段,系统趋于稳定,风险接受度内。

此动态演化分析不仅提供风险值随时间变化的曲线,更重要的是揭示了其背后的因果机制和状态转移过程,证明模型捕捉系统性、时序性风险的能力。

3.2 风险缓解策略

针对核心风险驱动因素(政策延迟、技术滞后)及关键事故类型(空域冲突、通信中断、导航偏移),构建多维度系统性风险缓解框架,具体策略如下:

- 1) 政策协同与标准统一。由 ICAO 牵头定期发布《真北过渡白皮书》,明确技术路线与责任主

体,建立“阶段达标-资金拨付”联动机制;按地理纬度差异制定差异化分阶段过渡时间表,辅以约束性条款保障各方履约。

2) 技术实施与设备升级。短期研发“真北-磁北”转换中间件实现无缝切换;中长期按机型寿命分级推进-新机型集成 GNSS-惯性导航系统(Inertial Navigation System,INS)真北方案,中期服役机型加装兼容模块,老旧机型逐步淘汰,破解技术代际断层。

3) 人员培训与应急响应。在飞行员、管制员培训中增设混合运行、GNSS 失效等核心场景高频模拟演练;制定标准化应急协议,明确处置流程,将备份系统激活等关键环节耗时控制在 30 s 内。

4) 环境冗余与抗干扰设计。极地等 GNSS 薄弱区域部署“惯导+星链”双冗余架构,定位误差控制在 0.1 nmile 内;整合地磁扰动监测数据,构建空间天气预警平台,支撑动态航路规划。

5) 长期维护与持续优化。成立国际技术联盟,搭建设备改造、故障案例、政策效能共享数据库;开发人工智能驱动优化系统,动态调整政策干预与技术升级节奏,实现闭环风险治理。

4 结 论

1) 政策延迟与技术适配滞后是引发空域冲突、通信中断与导航偏移等事故的关键驱动因素。动态模拟进一步揭示,通过分阶段设备升级与政策协调,可将关键风险从初始的高水平(空域冲突概率为 0.852)显著降低至长期稳定阶段的低水平(≤ 0.01)。

2) 在此基础上,提出民航导航真北过渡的三项原创策略,①建立“阶段达标-资金拨付”联动机制与差异化过渡时间表,以解决政策执行延迟;②实施基于机型寿命分级的“新集成、中加装、旧淘汰”技术迭代路径,规避设备代际冲突;③构建“惯导+低轨卫星”双冗余架构与人工智能动态治理体系,将导航误差锁定在 0.1 n mile 内并确保关键风险概率稳定低于 0.01。

3) 所构建的 STPA-FBN-DBN 建模框架由于缺乏实际运行数据支持,无法进行历史数据对比分析,当前模型仍依赖专家主观判断,未来可通过引入系统动力学方法、集成实时运行数据与人工智能优化机制,进一步提升模型的鲁棒性与预测能力。

参 考 文 献

[1] Pleter O T, Constantinescu C E. Study on the transition to true north in air navigation[J]. Aerospace, 2023, 10(11): DOI:10.3390/aerospace10110912.

[2] International Coordinate Council of Aerospace Industries Associations. ICCAIA true north whitepaper v. 1. 1: true north ICCAIA Ad-hoc group white paper v1. 1 [R/OL]. (2023-11-20). <https://iccaia.org/wp-content/uploads/2023/11/True-North-ICCAIA-White-Paper-v1.1-20Nov2023.pdf>.

[3] ICAO/ANB/OPS. Survey report survey on moving from a magnetic to a true north reference system for heading and tracking in aviation operations [R/OL]. (2023-11-20). https://www.navnin.nl/new/wp-content/uploads/2023/07/True-north-survey_AHRTAG_V1.pdf.

[4] Abdulkhaleq A, Wagner S, Leveson N. A comprehensive safety engineering approach for software-intensive systems based on STPA[J]. Procedia Engineering, 2015, 128:2-11.

[5] Krauss S S, Rejzek M, Hilbes C. Tool qualification considerations for tools supporting STPA[J]. Procedia Engineering, 2015, 128:15-24.

[6] Sahay R, Estay D A S, Meng W, et al. A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS[J]. Computers & Security, 2023, 128: DOI:10.1016/j.cose.2023.103179.

[7] Basnet S, Bahootoroody A, Montewka J, et al. Selecting cost-effective risk control option for advanced maritime operations; integration of STPA-BN-Influence diagram[J]. Ocean Engineering, 2023, 280: DOI:10.1016/j.oceaneng.2023.114631.

[8] 张子昂,张晓全. 基于 STPA 和模糊贝叶斯网络的大型无人驾驶航空器运行风险分析[J]. 航空工程进展, 2026, 17(1):72-80, 89.

Zhang Zi'ang, Zhang Xiaoquan. Operational risk analysis of large unmanned aerial vehicles based on STPA and fuzzy Bayesian network[J]. Advances in Aeronautical Science and Engineering, 2026, 17(1):72-80, 89.

[9] 王洁宁, 李保桢, 冀姗姗. 基于 STPA 和模糊 BN 的 AIDC 移交人误研究[J]. 中国安全科学学报, 2019, 29(9): 27-35.
Wang Jiening, Li Baoshen, Ji Shanshan. Study on human error in AIDC transfer based on STPA and fuzzy BN[J]. China Safety Science Journal, 2019, 29(9): 27-35.

[10] 席永涛, 刘鹏杰, 胡甚平, 等. 基于 STPA 和 FTPN 的海上自主水面船舶航行实时风险评估[J]. 中国安全科学学报, 2024, 34(8): 18-26.
Xi Yongtao, Liu Pengjie, Hu Shenping, et al. Real-time risk assessment for maritime autonomous surface ships based on STPA and FTPN[J]. China Safety Science Journal, 2024, 34(8): 18-26.

[11] Li Wei, Chen Weijiong, Hu Shenping, et al. Risk evolution model of marine traffic via STPA method and MC simulation: a case of MASS along coastal setting[J]. Ocean Engineering, 2023, 281: DOI: 10.1016/j.oceaneng.2023.114673.

[12] Lu Xin, Zeng Shengkui, Guo Jianbin, et al. An integrated method of extended STPA and BN for safety assessment of man-machine phased-mission system[J]. Reliability engineering & system safety, 2025, 253: DOI: 10.1016/j.res.2024.110569.

[13] 张玉磊, 朱德米. 重大决策社会稳定风险评估中的利益相关者参与: 行动逻辑与模式构建[J]. 上海行政学院学报, 2018, 19(5): 70-81.
Zhang Yulei, Zhu Demi. The stakeholder participation of major policy social stability risk assessment: action logic and pattern construction[J]. The Journal of Shanghai Administration Institute, 2018, 19(5): 70-81.

[14] 门茂林, 王智, 薛慧艳, 等. 真北定向测量方法及其对比分析[J]. 城市勘测, 2018(5): 135-137.
Men Maolin, Wang Zhi, Xue Huiyan, et al. Analysis and comparison of true north orientation measurement[J]. Urban Geotechnical Investigation & Surveying, 2018 (5): 135-137.

[15] Thomas J, Suo Dajiang. STPA-based method to identify and control feature interactions in large complex systems[J]. Procedia Engineering, 2015, 128: 12-14.

[16] Zhang Jixin, Zhang Shihao, Liang Zhengwei, et al. A risk assessment method based on DEMATEL-STPA and its application in safety risk evaluation of hydrogen refueling stations[J]. International Journal of Hydrogen Energy, 2024, 50: 889-902.

作者简介: 任杰 (1983—), 男, 山东平原人, 博士研究生, 讲师, 主要研究方向为空中交通流量管理、民航安全评估。E-mail: jren@cauc.edu.cn。

